SCHOOL OF PLANNING AND ARCHITECTURE

An 'Institution of National Importance' under the Act of Parliament
(Ministry of Human Resource Development, Government of India)
4, Block-B, Indraprastha Estate, New Delhi - 110002
Tel: 23724249 Fax: 011-23702383

Tender Fee Rs. 500/-
(Non-refundable)

NOTICE INVITED TENDER

Ref. No.: F.13-2/13/SPA(PSM) 10th August. 2015

Subject: **Wi-Fi Router is to be installed in the Department of Regional Planning Studio, Urban Design, Transport planning, Architectural Conservation & Physical planning of the School.**

Sealed items rate tender is invited for the Wi-Fi Router is to be installed in the Department of Regional planning Studio, Urban Design, Transport planning, Architectural Conservation & Physical planning of the School.

Tender forms/ documents may be downloaded from the website of the School i.e. www.spa.ac.in. The tenders must reach the undersigned on or before 25th August, 2015 by 1:00 p.m. and shall be opened on next day i.e. 26th August, 2015 at 12.00 noon. The Cost of the Tender document is Rs.500/- (Non-refundable) and the Earnest Money Deposit (EMD amounting to Rs. 11,000/- (Rupees Eleven thousand only) is required to be submitted. The bidders are required to go through the Terms and Conditions before submitting their tender / details at Annexure-A, Annexure-B, Annexure-C, Annexure-D (1 to 11 pages) and Annexure-E attached to the tender forms/documents.

The School reserves the right to reject any or all the tender without assigning any reason thereof. The School also reserves the right to award the services to one or more than one agencies. Incomplete and conditional tenders shall be rejected.

Sd/-

(Haresh Lalwani)
Section Officer
(PSM)
Email: spapsm@gmail.com
Ph: 23724249

General Terms and Conditions

a) All the correspondence regarding this tender should be addressed to the Section Officer (PSM) School of Planning and Architecture, 4 Block-B, I.P. Estate. New Delhi- 110002.

b) VAT as applicable may be shown separately in the tender.

c) The Bidder should be able to install the said material completely within **20 DAYS** from the receipt of the work order.

d) The Rates should include loading, unloading and transportation charges, if any.

…

Annexure-A

SCHOOL OF PLANNING AND ARCHITECTURE

Name of Work :- **Wi-Fi Router is to be installed in the Department of Regional Planning Studio, Urban Design, Transport planning, Architecture Conservation & Physical planning of the School.**

1. Due date of tender : _____
2. Opening time and date of tender : _____
3. Name, address of Firm/Agency and Telephone Nos. : _____
   _____
4. Registration No. of the Firm/Agency, if any : _____
5. Name, Designation, address and Telephone No. of Authorized person of Firm/Agency to deal with: : _____
   _____
6. Copy of PAN card iss by Income Tax Department and Copy previous three Financ Year's Income tax Return. (if available) : _____
7. Any other information : _____

This is to certify that I/We before signing this tender have read and fully understood all the terms and conditions contained herein and undertake myself/ourselves abide by them.

(Signature of the bidder)_____

Name & Address: _____

(With seal) _____

Annexure:-B

UNDERTAKING

To,

The Registrar,
School of Planning and Architecture,
4-Block-B, Indraprastha Estate,
New Delhi-110002

Sir,

i. I/We the undersigned, certify that I/we have gone through the terms and conditions mentioned in the tender documents and undertake to comply with them.

ii. It is further certified that the firm is acceptable and has not been blacklisted by any agency in India or abroad*.

Date:_____

Signature of the tenderer_____

with seal

Place:_____

Name of the tenderer:_____

with address _____

_____

_____

- Not applicable for Government agencies.

Annexure -C

Name of Work: - WI-Fi Router installation in the Department of Regional Planning, Urban Design, Transport Planning, Architecture Conservation & Physical Planning SPA New Delhi

Schedule Of Work					
S.No	Names of Items	Specification	Approx. Qty.	Tentative Rate per Unit/ Meter	Total Amount
1	52 Port Cisco Gigabit Managed Switch	Specification Enclosed	1 Unit		
2	28 Port Cisco Gigabit Managed Switch	Specification Enclosed	1 Unit		
3	Cisco Wireless Controller for minimum supporting 25 AP	Specification Enclosed	1 Unit		
4	CON-SNT-CT2525	Cisco Support for Controller	1 Unit		
5	Cisco Aironet AP	Specification Enclosed	6 unit		
6	CON-SNT-AIRCAP17	Cisco Support for AP	1 Unit		
7	Cable Manager	High quality PVC Cable Manager	5 Unit		
8	Cat 6 cable 305 meter cable Bundle(D-Link)	The following item shall be supplied and laid on actual requirement basis	4 Unit		
9	6U Mounting Rack (supported with 52 port Cisco switch)	Fully Loaded	1 Unit		
10	1Mtr Patch cord of Cat 6. (D-link)	Category-6 UTP CABLES	50 Unit		
11	3Mtr Patch cord of Cat 6. (D-link)	Category-6 UTP CABLES	50 Unit		
12	Cat 6 I/O set face plate with gang box (D-link)	Single port, Fully Shielded with metal cover for total EMI/RFI Protection, Support up to cat 6.	30 Unit		
13	Jack Panel	24 port Panel support up to Cat 6 cable Fully Loaded	3 unit		
14	PVC Batten (Size as per requirement)	The following item shall be supplied and laid on actual requirement basis	1000 Mtr.		
15	Supply, installation, testing and Commissioning charge				

Total

(Rupees……..)

(Including All Tax)

Signature _____
Name _____
Address _____

Seal of the Firm _____

Date: _____
Place: _____

Annexure D

Product Specifications of Wireless Controller

Item	Specification
Wireless Standards	IEEE 802.11a, 802.11ac, 802.11b, 802.11g, 802.11d, WMM/802.11e, 802.11h, 802.11k, 802.11n, 802.11r, 802.11u, 802.11w, 802.11ac
Wired/Switching/Routing	IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX specification, 1000BASE-T, and IEEE 802.1Q VLAN tagging
Data Request for Comments (RFCs)	● RFC 768 UDP ● RFC 791 IP ● RFC 2460 IPv6 (passthrough bridging mode only) ● RFC 792 ICMP ● RFC 793 TCP ● RFC 826 ARP ● RFC 1122 Requirements for Internet Hosts ● RFC 1519 CIDR ● RFC 1542 BOOTP ● RFC 2131 DHCP ● RFC 5415 CAPWAP Protocol Specification
Security Standards	● Wi-Fi Protected Access (WPA) ● IEEE 802.11i (WPA2, RSN) ● RFC 1321 MD5 Message-Digest Algorithm ● RFC 1851 The ESP Triple DES Transform ● RFC 2104 HMAC: Keyed Hashing for Message Authentication ● RFC 2246 TLS Protocol Version 1.0 ● RFC 2401 Security Architecture for the Internet Protocol ● RFC 2403 HMAC-MD5-96 within ESP and AH ● RFC 2404 HMAC-SHA-1-96 within ESP and AH ● RFC 2405 ESP DES-CBC Cipher Algorithm with Explicit IV ● RFC 2406 IP Encapsulating Security Payload (ESP) ● RFC 2407 Interpretation for ISAKMP ● RFC 2408 ISAKMP ● RFC 2409 IKE ● RFC 2451 ESP CBC-Mode Cipher Algorithms ● RFC 3280 Internet X.509 PKI Certificate and CRL Profile ● RFC 3602 The AES-CBC Cipher Algorithm and Its Use with IPsec ● RFC 3686 Using AES Counter Mode with IPsec ESP ● RFC 4347 Datagram Transport Layer Security ● RFC 4346 TLS Protocol Version 1.1
Encryption	● WEP and Temporal Key Integrity Protocol-Message Integrity Check (TKIP-MIC): RC4 40, 104 and 128 bits (both static and shared keys) ● Advanced Encryption Standard (AES): CBC, CCM, Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) ● DES: DES-CBC, 3DES ● Secure Sockets Layer (SSL) and Transport Layer Security (TLS): RC4 128-bit and RSA 1024- and 2048-bit ● DTLS: AES-CBC
Authentication, Authorization, and Accounting (AAA)	● IEEE 802.1X ● RFC 2548 Microsoft Vendor-Specific RADIUS Attributes ● RFC 2716 PPP EAP-TLS ● RFC 2865 RADIUS Authentication ● RFC 2866 RADIUS Accounting ● RFC 2867 RADIUS Tunnel Accounting ● RFC 3576 Dynamic Authorization Extensions to RADIUS ● RFC 3579 RADIUS Support for EAP ● RFC 3580 IEEE 802.1X RADIUS Guidelines ● RFC 3748 Extensible Authentication Protocol

	● Web-based authentication ● TACACS support for management users
Management	SNMP v1, v2c, v3 RFC 854 Telnet RFC 1155 Management Information for TCP/IP-Based Internets RFC 1156 MIB RFC 1157 SNMP RFC 1213 SNMP MIB II RFC 1350 TFTP RFC 1643 Ethernet MIB RFC 2030 SNTP RFC 2616 HTTP RFC 2665 Ethernet-Like Interface types MIB RFC 2674 Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual Extensions RFC 2819 RMON MIB RFC 2863 Interfaces Group MIB RFC 3164 Syslog RFC 3414 User-Based Security Model (USM) for SNMPv3 RFC 3418 MIB for SNMP RFC 3636 Definitions of Managed Objects for IEEE 802.3 MAUs Cisco private MIBs
Management Interfaces	● Designed for use with Cisco Wireless Control System ● Web-based: HTTP/HTTPS individual device manager ● Command-line interface: Telnet, SSH, serial port
Interfaces and Indicators	● Console port: RJ-45 connector ● Network: Four 1 Gbps Ethernet (RJ-45) ● LED indicators: Link Activity (each 1 Gigabit Ethernet port), Power, Status, Alarm
Physical and Environmental	Dimensions: 1.73 x 8.00 x 6.75 in. (43.9 x 203.2 x 271.5mm) Weight: 3.5 lbs (with power supply) Temperature: ● Operating: 32 to 104 °F (0 to 40°C) ● Storage: -13 to 158°F (-25 to 70°C) Humidity: ● Operating humidity: 10 to 95 percent, noncondensing ● Storage humidity: Up to 95 percent Power adapter: Input power: 100 to 240 VAC; 50/60 Hz Heat dissipation: 72 BTU/hour

Feature	Benefits
Scalability	● Supports up to 75 access points ● Supports up to 1000 clients
Ease of Deployment	● For quick and easy deployment Access Points can be connected directly to 2504 Wireless LAN Controller via two PoE (Power over Ethernet) ports
High Performance	● Wired-network speed and nonblocking performance for 802.11n and 802.11ac networks. Supports up to 1 Gbps throughput
RF Management	● Provides both real-time and historical information about RF interference impacting network performance across controllers, via systemwideCisco CleanAir® technology integration
Comprehensive End-to-End Security	● Offers CAPWAP-compliant Datagram Transport Layer Security (DTLS) encryption to help ensure full-line-rate encryption between access points and controllers across remote WAN/LAN links
End-to-end Voice	● SupportsUnified Communications for improved collaboration through messaging, presence, and conferencing ● Supports allCisco Unified Wireless IP Phones for cost-effective, real-time voice services
High-Performance Video	● Integrates Cisco VideoStream technology as part of the Cisco medianet framework to optimize the delivery of video applications across the WLAN
PCI Integration	● Part of Payment Card Industry (PCI) certified architecture, and are well-suited for retail customers who deploy transactional data applications such as scanners and kiosks
OfficeExtend	● Supports corporate wireless service for mobile and remote workers with secure wired tunnels to the Cisco Aironet® 600, 1130, 1140 or 3500 Series Access Points ● Extends the corporate network to remote locations with minimal setup and maintenance requirements ● Improves productivity and collaboration at remote site locations ● Separate service set identifier (SSID) tunnels allow both corporate and personal Internet access ● Reduced carbon dioxide emissions from a decrease in commuting ● Higher employee job satisfaction from ability to work at home ● Improves business resiliency by providing continuous, secure connectivity in the event of disasters, pandemics, or inclement weather
Enterprise Wireless Mesh	● Allows access points to dynamically establish wireless connections without the need for a physical connection to the wired network ● Available on select Cisco Aironet access points, Enterprise Wireless Mesh is ideal for warehouses, manufacturing floors, shopping centers, and any other location where extending a wired connection may prove difficult or aesthetically unappealing
Environmentally Responsible	● Organizations may choose to turn off access point radios to reduce power consumption during off-peak hours
Mobility, Security and Management for IPv6 & Dual-Stack Clients	● Secure, reliable wireless connectivity and consistent end-user experience ● Increased network availability by proactive blocking of known threats ● Equips administrators for IPv6 troubleshooting, planning, client traceability from a common wired and wireless management system
Guest Anchor and Wired Guest Access	● Supports up to 15 guest anchor Ethernet over IP (EoIP) tunnels forpath isolation of guest traffic from enterprise data traffic ● Extends the guest access services to the wired clients on par with other WLAN Controllers

Product Specifications for Access Point

Item	Specification
Supported wireless LAN controllers	controller supported
802.11n version 2.0 (and related) capabilities	● 3x3 MIMO with two spatial streams ● Maximal ratio combining (MRC) ● 802.11n and 802.11a/g beamforming ● 20- and 40-MHz channels ● PHY data rates up to 300 Mbps (40 MHz with 5 GHz) ● Packet aggregation: A-MPDU (Tx/Rx), A-MSDU (Tx/Rx) ● 802.11 Dynamic Frequency Selection (DFS) ● Cyclic shift diversity (CSD) support
802.11ac Wave 1 capabilities	● 3x3 MIMO with two spatial streams ● MRC ● 802.11ac-standard explicit beamforming ● 20-, 40-, and 80-MHz channels ● PHY data rates up to 867 Mbps (80 MHz in 5 GHz) ● Packet aggregation: A-MPDU (Tx/Rx), A-MSDU (Tx/Rx) ● 802.11 DFS ● CSD support
Data rates supported	802.11a: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps 802.11n data rates on 2.4 GHz:

MCS Index[1]	GI[2] = 800 ns 20-MHz Rate (Mbps)	GI = 400 ns 20-MHz Rate (Mbps)
0	6.5	7.2
1	13	14.4
2	19.5	21.7
3	26	28.9
4	39	43.3
5	52	57.8
6	58.5	65
7	65	72.2
8	13	14.4
9	26	28.9
10	39	43.3
11	52	57.8
12	78	86.7
13	104	115.6
14	117	130
15	130	144.4

802.11ac data rates (5 GHz):

MCS Index[3]	Spatial Streams	GI[4] = 800ns			GI = 400ns		
		20-MHz Rate (Mbps)	40-MHz Rate (Mbps)	80-MHz Rate (Mbps)	20-MHz Rate (Mbps)	40-MHz Rate (Mbps)	80-MHz Rate (Mbps)
0	1	6.5	13.5	29.3	7.2	15	32.5
1	1	13	27	58.5	14.4	30	65
2	1	19.5	40.5	87.8	21.7	45	97.5
3	1	26	54	117	28.9	60	130
4	1	39	81	175.5	43.3	90	195
5	1	52	108	234	57.8	120	260
6	1	58.5	121.5	263.3	65	135	292.5
7	1	65	135	292.5	72.2	150	325
8	1	78	162	351	86.7	180	390
9	1	-	180	390	-	200	433.3
0	2	13	27	58.5	14.4	30	65
1	2	26	54	117	28.9	60	130
2	2	39	81	175.5	43.3	90	195
3	2	52	108	234	57.8	120	260
4	2	78	162	351	86.7	180	390
5	2	104	216	468	115.6	240	520
6	2	117	243	526.5	130	270	585
7	2	130	270	585	144.4	300	650
8	2	156	324	702	173.3	360	780
9	2	-	360	780	-	400	866.7

Frequency band and 20-MHz operating channels

A (A regulatory domain):
- 2.412 to 2.462 GHz; 11 channels
- 5.180 to 5.320 GHz; 8 channels
- 5.500 to 5.700 GHz; 8 channels

(excludes 5.600 to 5.640 GHz)
- 5.745 to 5.825 GHz; 5 channels

C (C regulatory domain):
- 2.412 to 2.472 GHz; 13 channels
- 5.745 to 5.825 GHz; 5 channels

D (D regulatory domain):
- 2.412 to 2.462 GHz; 11 channels
- 5.180 to 5.320 GHz; 8 channels
- 5.745 to 5.825 GHz; 5 channels

E (E regulatory domain):
- 2.412 to 2.472 GHz; 13 channels
- 5.180 to 5.320 GHz; 8 channels
- 5.500 to 5.700 GHz; 8 channels

(excludes 5.600 to 5.640 GHz)

F (F regulatory domain):
- 2.412 to 2.472 GHz; 13 channels
- 5.745 to 5.805 GHz; 4 channels

H (H regulatory domain):
- 2.412 to 2.472 GHz; 13 channels

N (N regulatory domain):
- 2.412 to 2.462 GHz; 11 channels
- 5.180 to 5.320 GHz; 8 channels
- 5.745 to 5.825 GHz; 5 channels

Q (Q regulatory domain):
- 2.412 to 2.472 GHz; 13 channels
- 5.180 to 5.320 GHz; 8 channels
- 5.500 to 5.700 GHz; 11 channels

R (R regulatory domain):
- 2.412 to 2.472 GHz; 13 channels
- 5.180 to 5.320 GHz; 8 channels
- 5.660 to 5.805 GHz; 7 channels

S (S regulatory domain):
- 2.412 to 2.472 GHz; 13 channels
- 5.180 to 5.320 GHz; 8 channels
- 5.500 to 5.700 GHz; 11 channels
- 5.745 to 5.825 GHz; 5 channels

T (T regulatory domain):
- 2.412 to 2.462 GHz; 11 channels
- 5.280 to 5.320 GHz; 3 channels
- 5.500 to 5.700 GHz; 8 channels

(excludes 5.600 to 5.640 GHz)
- 5.745 to 5.825 GHz; 5 channels

	● 5.180 to 5.350 GHz; 8 channels ● 5.745 to 5.825 GHz; 5 channels I (I regulatory domain): ● 2.412 to 2.472 GHz; 13 channels ● 5.180 to 5.320 GHz; 8 channels K (K regulatory domain): ● 2.412 to 2.472 GHz; 13 channels ● 5.180 to 5.320 GHz; 8 channels ● 5.500 to 5.620 GHz; 7 channels ● 5.745 to 5.805 GHz; 4 channels	Z (Z regulatory domain): ● 2.412 to 2.462 GHz; 11 channels ● 5.180 to 5.320 GHz; 8 channels ● 5.500 to 5.700 GHz; 8 channels (excludes 5.600 to 5.640 GHz) ● 5.745 to 5.825 GHz; 5 channels
Maximum number of nonoverlapping channels	2.4 GHz ● 802.11b/g: ◦ 20 MHz: 3 ● 802.11n: ◦ 20 MHz: 3	5 GHz ● 802.11a: ◦ 20 MHz: 24 ● 802.11n: ◦ 20 MHz: 24 ◦ 40 MHz: 11 ● 802.11ac: ◦ 20 MHz: 24 ◦ 40 MHz: 11 ◦ 80 MHz: 5
Receive sensitivity	● 802.11b (CCK) ◦ -101 dBm @ 1 Mbps ◦ -99 dBm @ 2 Mbps ◦ -93 dBm @ 5.5 Mbps ◦ -90 dBm @ 11 Mbps	● 802.11g (non HT20) ◦ -93 dBm @ 6 Mbps ◦ -92 dBm @ 9 Mbps ◦ -92 dBm @ 12 Mbps ◦ -91 dBm @ 18 Mbps ◦ -88 dBm @ 24 Mbps ◦ -85 dBm @ 36 Mbps ◦ -80 dBm @ 48 Mbps ◦ -79 dBm @ 54 Mbps	● 802.11a (non HT20) ◦ -93 dBm @ 6 Mbps ◦ -92 dBm @ 9 Mbps ◦ -92 dBm @ 12 Mbps ◦ -91 dBm @ 18 Mbps ◦ -88 dBm @ 24 Mbps ◦ -85 dBm @ 36 Mbps ◦ -80 dBm @ 48 Mbps ◦ -79 dBm @ 54 Mbps
	2.4 GHz ● 802.11n (HT20) ◦ -93 dBm @ MCS0 ◦ -92 dBm @ MCS1 ◦ -90 dBm @ MCS2 ◦ -87 dBm @ MCS3 ◦ -84 dBm @ MCS4 ◦ -79 dBm @ MCS5 ◦ -78 dBm @ MCS6 ◦ -77 dBm @ MCS7 ◦ -92 dBm @ MCS8 ◦ -90 dBm @ MCS9 ◦ -88 dBm @ MCS10 ◦ -85 dBm @ MCS11 ◦ -82 dBm @ MCS12 ◦ -78 dBm @ MCS13 ◦ -76 dBm @ MCS14 ◦ -75 dBm @ MCS15		5 GHz ● 802.11n (HT20) ◦ -93 dBm @ MCS0 ◦ -92 dBm @ MCS1 ◦ -90 dBm @ MCS2 ◦ -87 dBm @ MCS3 ◦ -84 dBm @ MCS4 ◦ -80 dBm @ MCS5 ◦ -78 dBm @ MCS6 ◦ -77 dBm @ MCS7 ◦ -92 dBm @ MCS8 ◦ -90 dBm @ MCS9 ◦ -88 dBm @ MCS10 ◦ -85 dBm @ MCS11 ◦ -82 dBm @ MCS12 ◦ -77 dBm @ MCS13 ◦ -76 dBm @ MCS14 ◦ -74 dBm @ MCS15	5 GHz ● 802.11n (HT40) ◦ -90 dBm @ MCS0 ◦ -88 dBm @ MCS1 ◦ -87 dBm @ MCS2 ◦ -84 dBm @ MCS3 ◦ -81 dBm @ MCS4 ◦ -76 dBm @ MCS5 ◦ -75 dBm @ MCS6 ◦ -74 dBm @ MCS7 ◦ -89 dBm @ MCS8 ◦ -87 dBm @ MCS9 ◦ -85 dBm @ MCS10 ◦ -82 dBm @ MCS11 ◦ -78 dBm @ MCS12 ◦ -74 dBm @ MCS13 ◦ -73 dBm @ MCS14 ◦ -71 dBm @ MCS15

802.11ac Receive Sensitivity

802.11ac (non HT80)
- -86 dBm @ 6 Mbps
- -74 dBm @ 54 Mbps

MCS Index[5]	Spatial Streams	VHT20	VHT40	VHT80	VTH20-STBC	VHT40-STBC	VHT80-STBC
0	1	-92 dBm	-89 dBm	-85 dBm	-92 dBm	-89 dBm	-85 dBm
8	1	-73 dBm			-73 dBm		
9	1		-68 dBm	-65 dBm		-68 dBm	-65 dBm
0	2	-91 dBm	-87 dBm	-84 dBm			
8	2	-71 dBm					
9	2		-66 dBm	-62 dBm			

Maximum transmit power	2.4 GHz ● 802.11b ◦ 22 dBm, 3 antennas ● 802.11g ◦ 22 dBm, 3 antennas ● 802.11n (HT20) ◦ 22 dBm, 3 antennas	5 GHz ● 802.11a ◦ 22 dBm, 3 antennas ● 802.11n (HT20) ◦ 22 dBm, 3 antennas ● 802.11n (HT40) ◦ 22 dBm, 3 antennas ● 802.11ac ◦ non-HT80: 22 dBm, 3 antennas ◦ VHT20 22 dBm, 3 antennas ◦ VHT40: 22 dBm, 3 antennas ◦ VHT80: 22 dBm, 3 antennas ◦ VHT20-STBC: 22 dBm, 3 antennas ◦ VHT40-STBC: 22 dBm, 3 antennas ◦ VHT80-STBC: 22 dBm, 3 antennas
Available transmit power settings	2.4 GHz ● 22 dBm (160 mW) ● 19 dBm (80 mW) ● 16 dBm (40 mW) ● 13 dBm (20 mW) ● 10 dBm (10 mW) ● 7 dBm (5 mW) ● 4 dBm (2.5 mW) ● 2 dBm (1.25 mW)	5 GHz ● 22 dBm (160 mW) ● 19 dBm (80 mW) ● 16 dBm (40 mW) ● 13 dBm (20 mW) ● 10 dBm (10 mW) ● 7 dBm (5 mW) ● 4 dBm (2.5 mW) ● 1 dBm (1.25 mW)
Integrated antenna	● 2.4 GHz, gain 4 dBi, internal omni, horizontal beamwidth 360° ● 5 GHz, gain 4 dBi, internal omni, horizontal beamwidth 360°	
Interfaces	● 2x10/100/1000BASE-T autosensing (RJ-45) ● Management console port (RJ-45)	
Indicators	● Status LED indicates boot loader status, association status, operating status, boot loader warnings, boot loader errors	
System memory	● 512 MB DRAM ● 64 MB flash	

Input power requirements	44 to 57 VDC ● Power supply and power injector: 100 to 240 VAC; 50 to 60 Hz
Power draw	15W
Powering options	● 802.3at PoE+ ● Enhanced PoE ● power injectors ● local power supply
Warranty	Limited lifetime hardware warranty
	● IEEEstandards: ◦ IEEE 802.11a/b/g, 802.11n, 802.11h, 802.11d ◦ IEEE 802.11ac Draft 5 ● Security: ◦ 802.11i, Wi-Fi Protected Access 2 (WPA2), WPA ◦ 802.1X ◦ Advanced Encryption Standards (AES), Temporal Key Integrity Protocol (TKIP) ● Extensible Authentication Protocol (EAP) types: ◦ EAP-Transport Layer Security (TLS) ◦ EAP-Tunneled TLS (TTLS) or Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAPv2) ◦ Protected EAP (PEAP) v0 or EAP-MSCHAPv2 ◦ EAP-Flexible Authentication via Secure Tunneling (FAST) ◦ PEAP v1 or EAP-Generic Token Card (GTC) ◦ EAP-Subscriber Identity Module (SIM) ● Multimedia: ◦ Wi-Fi Multimedia (WMM) ● Other: ◦ FCC Bulletin OET-65C ◦ RSS-102

Feature	**Benefit**
802.11ac Wave 1 support with 3x3 multiple input and multiple output (MIMO) and two spatial streams	Delivers higher rates over a greater range for more capacity and reliability than competing access points. Provides up to three times more bandwidth than 802.11n networks.
Cisco CleanAir® Express Spectrum Intelligence	Detects RF interference and provides basic spectrum analysis capabilities while simplifying ongoing operations across 20-, 40-, and 80-MHz-wide channels
Optimized access point roaming	Directs client devices to associate with the access point in their coverage range, offering the fastest data rate available
MIMO equalization	Boosts uplink performance and reliability by reducing the impact of signal fade

28 Port and 52 Port Gigabit Ethernet Switch Specifications	
Layer 2	
Spanning Tree Protocol (STP)	Standard 802.1d Spanning Tree support
	Fast convergence using 802.1w (Rapid Spanning Tree [RSTP]), enabled by default
	8 instances are supported
	Multiple Spanning Tree instances using 802.1s (MSTP)
Port grouping	Support for IEEE 802.3ad Link Aggregation Control Protocol (LACP)
	● Up to 8 groups
	● Up to 8 ports per group with 16 candidate ports for each (dynamic) 802.3ad link aggregation
VLAN	Support for up to 4096 VLANs simultaneously Port-based and 802.1Q tag-based VLANs MAC-based VLAN
	Management VLAN
	Private VLAN Edge (PVE), also known as protected ports, with multiple uplinks
	Guest VLAN Unauthenticated VLAN
	Dynamic VLAN assignment via Radius server along with 802.1x client authentication
	CPE VLAN
Voice VLAN	Voice traffic is automatically assigned to a voice-specific VLAN and treated with appropriate levels of QoS.
	Auto voice capabilities deliver network-wide zero touch deployment of voice endpoints and call control devices.
Multicast TV VLAN	Multicast TV VLAN allows the single multicast VLAN to be shared in the network while subscribers remain in separate VLANs (Also known as MVR)
Q-in-Q VLAN	VLANs transparently cross a service provider network while isolating traffic among customers
Generic VLAN Registration Protocol (GVRP)/Generic Attribute Registration Protocol (GARP)	Protocols for automatically propagating and configuring VLANs in a bridged domain
Unidirectional Link Detection (UDLD)	UDLD monitors physical connection to detect unidirectional links caused by incorrect wiring or cable/port faults to prevent forwarding loops and blackholing of traffic in switched networks
Dynamic Host Configuration Protocol (DHCP) Relay at Layer 2	Relay of DHCP traffic to DHCP server in different VLAN. Works with DHCP Option 82
Internet Group Management Protocol (IGMP) versions 1, 2, and 3 snooping	IGMP limits bandwidth-intensive multicast traffic to only the requesters; supports 1K multicast groups (source-specific multicasting is also supported)
IGMP Querier	IGMP querier is used to support a Layer 2 multicast domain of snooping switches in the absence of a multicast router
Head-of-line (HOL) blocking	HOL blocking prevention
Jumbo Frames	Up to 9K (9216) bytes
Layer 3	
IPv4 routing	Wirespeed routing of IPv4 packets
	Up to 512 static routes and up to 128 IP interfaces
Classless Inter-Domain Routing (CIDR)	Support for CIDR

Layer 3 Interface	Configuration of layer 3 interface on physical port, LAG, VLAN interface or Loopback interface
DHCP relay at Layer 3	Relay of DHCP traffic across IP domains
User Datagram Protocol (UDP) relay	Relay of broadcast information across Layer 3 domains for application discovery or relaying of BootP/DHCP packets
DHCP Server	Switch functions as an IPv4 DHCP Server serving IP addresses for multiple DHCP pools/scopes
	Support for DHCP options
Security	
Secure Shell (SSH) Protocol	SSH is a secure replacement for Telnet traffic. SCP also uses SSH. SSH v1 and v2 are supported
Secure Sockets Layer (SSL)	SSL support: Encrypts all HTTPS traffic, allowing highly secure access to the browser-based management GUI in the switch
IEEE 802.1X (Authenticator role)	802.1X: RADIUS authentication and accounting, MD5 hash; guest VLAN; unauthenticated VLAN, single/multiple host mode and single/multiple sessions
	Supports time-based 802.1X Dynamic VLAN assignment
Web Based Authentication	Web based authentication provides network admission control through web browser to any host devices and operating systems.
STP Bridge Protocol Data Unit (BPDU) Guard	A security mechanism to protect the network from invalid configurations. A port enabled for BPDU Guard is shut down if a BPDU message is received on that port.
STP Root Guard	This prevents edge devices not in the network administrator's control from becoming Spanning Tree Protocol root nodes.
DHCP snooping	Filters out DHCP messages with unregistered IP addresses and/or from unexpected or untrusted interfaces. This prevents rogue devices from behaving as a DHCP Server.
IP Source Guard (IPSG)	When IP Source Guard is enabled at a port, the switch filters out IP packets received from the port if the source IP addresses of the packets have not been statically configured or dynamically learned from DHCP snooping. This prevents IP Address Spoofing.
Dynamic ARP Inspection (DAI)	The switch discards ARP packets from a port if there is no static or dynamic IP/MAC bindings or if there is a discrepancy between the source or destination address in the ARP packet. This prevents man-in-the-middle attacks.
IP/Mac/Port Binding (IPMB)	The features (DHCP Snooping, IP Source Guard, and Dynamic ARP Inspection) above work together to prevent DOS attacks in the network, thereby increasing network availability.
Secure Core Technology (SCT)	Ensures that the switch will receive and process management and protocol traffic no matter how much traffic is received.
Secure Sensitive Data (SSD)	A mechanism to manage sensitive data (such as passwords, keys, etc) securely on the switch, populating this data to other devices, and secure autoconfig. Access to view the sensitive data as plaintext or encrypted is provided according to the user configured access level and the access method of the user.
Layer 2 isolation Private VLAN Edge (PVE) with community VLAN	PVE (also known as protected ports) provides Layer 2 isolation between devices in the same VLAN, supports multiple uplinks.
Port security	The ability to lock Source MAC addresses to ports, and limits the number of learned MAC
	addresses.
RADIUS/TACACS+	Supports RADIUS and TACACS authentication. Switch functions as a client.
Storm control	Broadcast, multicast, and unknown unicast
RADIUS accounting	The RADIUS accounting functions allow data to be sent at the start and end of services, indicating the amount of resources (such as time, packets, bytes, and so on) used during the session.
DoS prevention	Denial-of-Service (DOS) attack prevention
	Support for up to 512 rules

ACLs	Drop or rate limit based on source and destination MAC, VLAN ID or IP address, protocol, port, differentiated services code point (DSCP)/IP precedence, TCP/UDP source and destination ports,
	802.1p priority, Ethernet type, Internet Control Message Protocol (ICMP) packets, IGMP packets, TCP flag, Time-based ACLs supported.
Quality of Service	
Priority levels	4 hardware queues
Scheduling	Strict priority and weighted round-robin (WRR)
	Queue assignment based on DSCP and class of service (802.1p/CoS)
Class of service	Port based; 802.1p VLAN priority based; IPv4/v6 IP precedence/type of service (ToS)/DSCP based; Differentiated Services (DiffServ); classification and re-marking ACLs, trusted QoS.
Rate limiting	Ingress policer; egress shaping and rate control; per VLAN, per port, and flow based.
Congestion avoidance	A TCP congestion avoidance algorithm is required to minimize and prevent global TCP loss synchronization.
Standards	
Standards	IEEE 802.3 10BASE-T Ethernet, IEEE 802.3u 100BASE-TX Fast Ethernet, IEEE 802.3ab 1000BASE-T Gigabit Ethernet, IEEE 802.3ad LACP, IEEE 802.3z Gigabit Ethernet, IEEE 802.3x Flow Control, IEEE 802.1D (STP, GARP, and GVRP),IEEE 802.1Q/p VLAN, IEEE 802.1w RSTP, IEEE 802.1s Multiple STP, IEEE 802.1X Port Access Authentication, IEEE 802.3af, IEEE 802.3at, RFC 768, RFC 783, RFC 791, RFC 792, RFC 793, RFC 813, RFC 879, RFC 896, RFC 826, RFC 854, RFC 855, RFC 856, RFC 858, RFC 894, RFC 919, RFC 922, RFC 920, RFC 950, RFC 1042, RFC 1071, RFC 1123, RFC 1141, RFC 1155, RFC 1157, RFC 1350, RFC 1533, RFC 1541, RFC 1624, RFC 1700, RFC 1867, RFC 2030, RFC 2616, RFC 2131, RFC 2132, RFC 3164, RFC 3411, RFC 3412, RFC 3413, RFC 3414, RFC 3415, RFC 2576, RFC 4330, RFC 1213, RFC 1215, RFC 1286, RFC 1442, RFC 1451, RFC 1493, RFC 1573, RFC 1643, RFC 1757, RFC 1907, RFC 2011, RFC 2012, RFC 2013, RFC 2233, RFC 2618, RFC 2665, RFC 2666, RFC 2674, RFC 2737, RFC 2819, RFC 2863, RFC 1157, RFC 1493, RFC 1215, RFC 3416
IPv6	
IPv6	IPv6 host mode
	IPv6 over Ethernet Dual IPv6/IPv4 stack
	IPv6 neighbor and router discovery (ND) IPv6 stateless address auto-configuration
	Path maximum transmission unit (MTU) discovery
	Duplicate address detection (DAD) ICMP version 6
	IPv6 over IPv4 network with Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) support
	USGv6 and IPv6 Gold Logo certified
IPv6 QoS	Prioritize IPv6 packets in hardware
IPv6 ACL	Drop or rate limit IPv6 packets in hardware
IPv6 First Hop Security	RA guard
	ND inspection
	DHCPv6 guard
	Neighbor binding table (Snooping and static entries)
	Neighbor binding integrity check
Multicast Listener Discovery	Deliver IPv6 multicast packets only to the required receivers
(MLD v1/2) snooping	
IPv6 applications	Web/SSL, Telnet server/SSH, ping, traceroute, Simple Network Time Protocol (SNTP), Trivial File Transfer Protocol (TFTP), SNMP, RADIUS, syslog, DNS client, Telnet Client, DHCP Client, DHCP Autoconfig, IPv6 DHCP Relay, TACACS
IPv6 RFCs supported	RFC 4443 (which obsoletes RFC2463) – ICMP version 6
	RFC 4291 (which obsoletes RFC 3513) – IPv6 address architecture
	RFC 4291 – IPv6 addressing architecture
	RFC 2460 – IPv6 specification
	RFC 4861 (which obsoletes RFC 2461) – Neighbor discovery for IPv6
	RFC 4862 (which obsoletes RFC 2462) – IPv6 stateless address auto-configuration

	RFC 1981 – Path MTU discovery
	RFC 4007 – IPv6 scoped address architecture
	RFC 3484 – Default address selection mechanism
	RFC 5214 (which obsoletes RFC 4214) – ISATAP tunneling RFC 4293 – MIB IPv6: Textual conventions and general group RFC 3595 – Textual conventions for IPv6 flow label
Management	
Web user interface	Built-in switch configuration utility for easy browser-based device configuration (HTTP/HTTPS). Supports configuration, system dashboard, system maintenance, and monitoring.
SNMP	SNMP versions 1, 2c, and 3 with support for traps, and SNMP version 3 user-based security model (USM)
Remote Monitoring (RMON)	Embedded RMON software agent supports 4 RMON groups (history, statistics, alarms, and events) for enhanced traffic management, monitoring, and analysis
IPv4 and IPv6 dual stack	Coexistence of both protocol stacks to ease migration
	● Web browser upgrade (HTTP/HTTPS) and TFTP and upgrade over SCP running over SSH
	● Upgrade can be initiated through console port as well
	● Dual images for resilient firmware upgrades
Port mirroring	Traffic on a port can be mirrored to another port for analysis with a network analyzer or RMON probe. Up to 8 source ports can be mirrored to one destination port. A single session is supported.
VLAN mirroring	Traffic from a VLAN can be mirrored to a port for analysis with a network analyzer or RMON probe. Up to 8 source VLANs can be mirrored to one destination port. A single session is supported.
DHCP (Options 12, 66, 67, 82, 129, and 150)	DHCP Options facilitate tighter control from a central point (DHCP server) to obtain IP address, auto-configuration (with configuration file download), DHCP relay, and hostname.
Secure Copy (SCP)	Securely transfer files to and from the switch
Autoconfiguration with Secure Copy (SCP) file download	Enables secure mass deployment with protection of sensitive data
Text-editable config files	Config files can be edited with a text editor and downloaded to another switch, facilitating easier mass deployment
Smartports	Simplified configuration of QoS and security capabilities
Auto Smartports	Applies the intelligence delivered through the Smartport roles and applies it automatically to the port based on the devices discovered over CDP or LLDP-MED. This facilitates zero touch deployments.
Textview CLI	Scriptable command-line interface. A full CLI as well as a menu-based CLI is supported. User privilege levels 1, 7, and 15 is supported for the CLI.
Cloud services	Support for Cisco Small Business FindIT Network and Cisco OnPlus
Localization	Localization of GUI and documentation into multiple languages
Other management	Traceroute; single IP management; HTTP/HTTPS; SSH; RADIUS; port mirroring; TFTP upgrade; DHCP client; BOOTP; SNTP; Xmodem upgrade; cable diagnostics; ping; syslog; Telnet client (SSH secure support)
Time-based port operation	Link up or down based on user-defined schedule (when the port is administratively up)
Login banner	Configurable multiple banners for web as well as CLI
Power Efficiency	
EEE Compliant (802.3az)	Supports 802.3az on all copper ports (SG300 models)
Energy Detect	Automatically turns off power off on Gigabit Ethernet and 10/100 RJ-45 port when detecting link down
	Active mode is resumed without loss of any packets when the switch detects the link up

Cable length detection	Adjusts the signal strength based on the cable length for Gigabit Ethernet models. Reduces the power consumption for cables shorter than 10m.
Disable port LEDs	LEDs can be manually turned off to save on Energy
General	
Jumbo frames	Frame sizes up to 9K (9216) bytes supported on 10/100 and Gigabit interfaces
MAC table	Up to 16K (16384) MAC addresses
Discovery	
Bonjour	The switch advertises itself using the Bonjour protocol.
Link Layer Discovery Protocol (LLDP) (802.1ab) with LLDP-MED extensions	LLDP allows the switch to advertise its identification, configuration, and capabilities to neighboring devices that store the data in a MIB. LLDP-MED is an enhancement to LLDP that adds the extensions needed for IP phones.
Cisco Discovery Protocol	The switch advertises itself using the Cisco Discovery Protocol. It also learns the connected device and its characteristics via CDP.
Buttons	Reset button
Cabling type	Unshielded twisted pair (UTP) Category 5 or better for 10BASE-T/100BASE-TX; UTP Category 5
	Ethernet or better for 1000BASE-T
LEDs	System, Link/Act, PoE, Speed, LED power saving option
Flash	16 MB
CPU memory	128 MB
Warranty	Limited lifetime with next business day advance replacement (where available)

Annexure E

SCOPE OF WORK

New installation and integration with existing LAN setup includes but not limited to the following tentative work:

1. Indoor UTP Cable Laying through PVC Pipe, Casing including all materials.

2. Preparation of Actual Bill of Material based on Survey and SPA requirements.

3. Installation of IO/Crimping/Patch Panel/ Rack/ Switch and System Integration.

4. Laying and Termination of CAT6 UTP Cable. All cabling must be “structured”.

5. Network Documentation (on Paper and CD).

6. All the CD’s, operational manuals, stationery and similar accessories made available by Equipment vendor would be handed over to SPA after installation work is over.

7. Labelling of Cables, I/Os, Jack Panel, Switches for new connections

8. Repair/Refurnishing work owing to damage caused due to cabling or any other work related to this Project. There should not be any hanging or uncovered wire.

9. Patch cord should be of branded company and factory crimped.

10. Equipment furnished shall be complete in every respect with all mountings, fittings, fixtures and standard accessories normally provided with such equipment and/or needed for erection, completion and safe operation of the equipment as required by applicable codes though they may not have been specifically detailed in the tender document.

11 The Bidder shall be responsible for providing all materials, equipment's, and services, specified or otherwise, which are required to fulfil the intent of ensuring operability, maintainability, and reliability of the complete equipment covered under this specification within his quoted price. This work shall be in compliance with all applicable standards, statutory regulations and safety requirements in force of the date of award of this contract.

12 The bidder shall also be responsible for deputing qualified personnel for installation, testing, commissioning and tackles for completing the scope of work.

13 The installation of equipment shall be accepted only after installation tests are over.

14. The bidder should ensure while installation of LAN, day-to-day functioning of official work and existing network setup/connectivity/internet connectivity should not get disrupted.

15. The bidder’s proposal shall include the list of tools (such as crimping tool, Krone punch tool) other accessories, which are required for installation of the connection. No separate charges for fixing/crimping/other connection charges would be paid by SPA

16. The scope covers design/development of a suitable architecture/layout of the proposed networking system, preparation of bill of materials, pre-dispatch inspection/testing, packing and forwarding, transportation, insurance and carrying out further activities at sites viz. unloading, storage, (space to be provided by the SPA) further handling, erection, testing and commissioning including successful completion of acceptance tests and any other services specified.

17. SPA reserves the right for quantity variation due to increase/decrease in. The bidder shall also provide all required equipment which may not be specifically stated herein but are required to meet the intent of ensuring completeness, maintainability and reliability of the total system covered under this specification, including integration and interoperability with the existing LAN.

18. Scope of Work shall also include

    a. Powering on equipment after ensuring correctness of terminations interfaces and power supply and making the system ready for testing and commissioning.

    b. Testing of LAN Cables after laying, terminations and ferruling at both the ends. All testing tools and instruments shall be brought by the bidder and taken back after the testing.

    c. Configuration of the equipment as per the requirements of SPA including Network segmentation and Network Monitoring though network management s/w.

    d. Site acceptance tests to establish satisfactory performance of the equipment's as per specs.

    e. Onsite warranty for all Installation and Hardware delivered for minimum one year and extended as per OEM guarantee/warranty offered.

19 . In case, the quantity of laying cables or fixing wall mount sockets etc. exceeds or is less than the quantity in bid price schedule, the payment for the executed quantity shall be paid on pro-rata basis, for the actual quantities consumed.